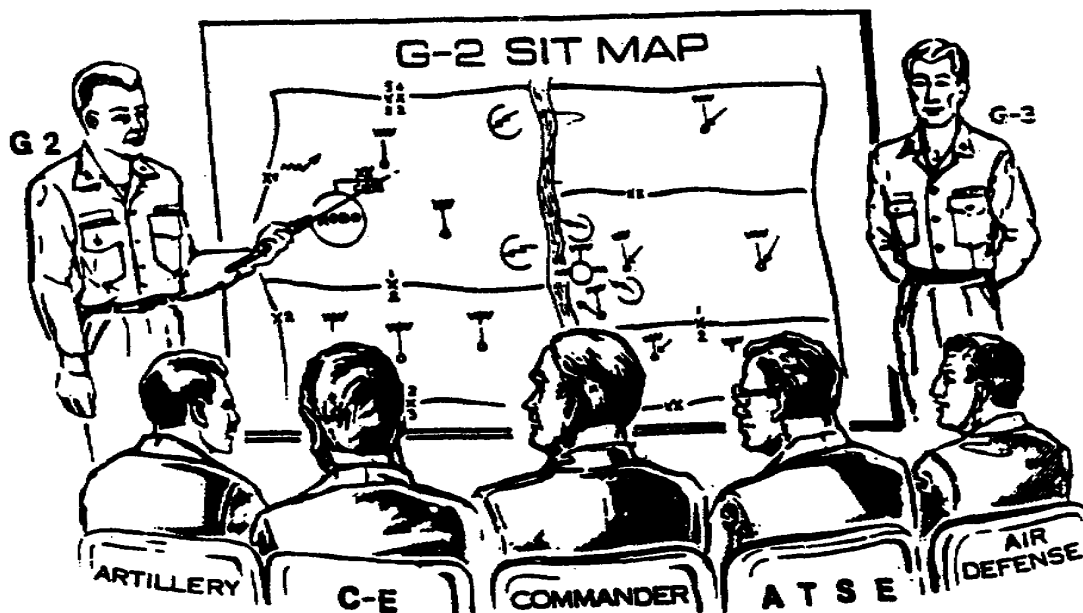


US ARMY INTELLIGENCE CENTER

INTELLIGENCE OFFICER RESPONSIBILITIES



THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT
ARMY CORRESPONDENCE COURSE PROGRAM

A
I
P
D

READINESS/
PROFESSIONALISM



THRU
GROWTH

INTELLIGENCE OFFICER RESPONSIBILITIES

Subcourse Number IT 0423

EDITION B

United States Army Intelligence Center and Fort Huachuca
Fort Huachuca, Arizona 85613-6000

6 Credit Hours

Edition Date: October 1999

Subcourse Overview

This subcourse provides information on the responsibilities of the intelligence officer. It covers the aspects of intelligence needed to be an effective intelligence officer.

There are no prerequisites for this subcourse. This subcourse reflects the doctrine which was current at the time the subcourse was prepared. In your own work situation, always refer to the latest publications.

The words "he," "her," and "men," when used in this publication, represent both the masculine and feminine gender unless otherwise stated.

TERMINAL LEARNING OBJECTIVE:

- ACTIONS:** You will be able to conduct intelligence training, intelligence planning, combat reconnaissance and surveillance, analysis of the area operation, and procure and distribute maps.
- CONDITIONS:** You will be given narrative information and illustrations of sample formats from FM 34-1, FM 34-2, FM 34-02-1, FM 34-3, FM 34-130, and FM 101-5.
- STANDARDS:** To demonstrate competency of this task, you must achieve a minimum of 70% on the subcourse examination.

TABLE OF CONTENTS

| Section | Page |
|---|------|
| Subcourse Overview | i |
| LESSON 1: ARMY UNIVERSAL TASK LIST (AUTL) | 1-1 |
| IEW and Force Projection | 1-2 |
| The Army Universal Task List | 1-2 |
| Training the IEW BOS | 1-3 |
| The Levels of Intelligence | 1-3 |
| Intelligence Disciplines and Functions | 1-4 |
| Characteristics of Effective Intelligence | 1-4 |
| The Intelligence Cycle | 1-5 |
| Practice Exercise | 1-7 |
| Answer Key and Feedback | 1-8 |
| LESSON 2: INTELLIGENCE PREPARATION OF THE BATTLEFIELD | 2-1 |
| IPB is a four step process | 2-2 |
| Practice Exercise | 2-15 |
| Answer Key and Feedback | 2-16 |
| LESSON 3: IPB AND ANALYSIS IN MILITARY STABILITY AND SUPPORT OPERATIONS | 3-1 |
| Stability and Support Operations | 3-2 |
| IPB Steps Remain the Same | 3-2 |
| Practice Exercise | 3-11 |
| Answer Key and Feedback | 3-12 |
| LESSON 4: INTRODUCTION TO THE RESPONSIBILITIES OF THE GARRISON INTELLIGENCE OFFICER | 4-1 |
| PART A - Physical Security | 4-2 |
| PART B - Information Security | 4-4 |
| Practice Exercise | 4-9 |
| Answer Key and Feedback | 4-10 |

LESSON 1

ARMY UNIVERSAL TASK LIST (AUTL)

Critical Tasks: None

OVERVIEW

LESSON DESCRIPTION:

This lesson will provide the student with an introduction to the Intelligence Battlefield Operating Systems (BOS). It includes the role of the commander, the levels of intelligence, the six primary tasks of intelligence, the disciplines and functions of intelligence, and the intelligence cycle. This lesson prepares the student for the following in this subcourse.

TERMINAL LEARNING OBJECTIVE:

TASK: You will be able to describe the intelligence BOS.

CONDITIONS: You will be given narrative information and illustrations of sample formats from FM 34-1, FM 34-3, and local standard operating procedures (SOPs).

STANDARDS: You will be able to describe the intelligence BOS and the fundamentals of Intelligence and Electronic Warfare (IEW) operation.

REFERENCES: The material contained in this lesson was derived from the following publications:

FM 34-1
FM 34-3

INTRODUCTION

Intelligence supports the Army as a whole through the Intelligence BOS. The Intelligence BOS is a flexible and tailorable architecture of procedures, personnel, organizations, and equipment that responds to the intelligence needs of commanders at all echelons. The Intelligence BOS architecture provides specific intelligence and communications structures at each echelon from the national level through the tactical level. These structures includes intelligence organizations and procedures for collecting, processing, analyzing, and delivering intelligence to decision makers who need it. Effective communications connectivity and automation are essential components of this architecture.

The Commander-Drives Intelligence. The role of the commander is a critical one to the success of the IEW BOS. To properly function, the IEW BOS must be directed by the commander, who should clearly articulate his intent, his intelligence needs, and the elements of the threat that are to be targeted. This direction should focus intelligence operations. The commander must also continually ensure that the IEW BOS is a leveraged, seamless part of the total combined arms

effort. Lastly, the commander must understand the limitations of the IEW BOS; it requires focus, it is a limited resource, it requires adequate communications support, and it reduces uncertainty on the battlefield but does not eliminate it.

Intelligence Synchronization. Intelligence synchronization is a continuous process that keeps the intelligence cycle and IEW operations tied to the commander's critical decisions and concept of operations.

Split-Based Operations. In split-based operations, the commander deploys small, flexible, tactically tailored IEW organizations into the Area of Operations (AO). He supports these elements with access to intelligence databases and systems, including national assets, outside the AO.

Tactical Tailoring. Tactical tailoring demands the right mix of IEW systems in the right numbers be deployed to support every US operation. It is influenced by a number of factors, including deployability, host nation intelligence capabilities, unit integrity, and logistics sustainability.

Broadcast Dissemination. Army intelligence strives to provide a "common" picture of the battlefield to deployed units. One of the most important means of achieving this is through the broadcast of intelligence to multiple echelons. There are numerous advantages to this means of dissemination, including the avoidance of bottlenecks and a reduction in the number of sensor systems that have to be deployed.

The Intelligence and Electronic Warfare (IEW) Battlefield Operating System (BOS). IEW is one of the US Army's BOS. It supports the other BOS, namely maneuver, fire support, air defense artillery, and combat service support, by providing intelligence products that respond to the intelligence needs of commanders from the national to tactical levels during peace and war.

As such, the mission of Army Intelligence is to provide timely, relevant, accurate, and synchronized IEW support to tactical, operational and strategic commanders across the range of military operations. In order to achieve this, military intelligence (MI) has the METL (M -mission, E -Essential, T -Task, L -List) for the intel corps. These are:

- **Providing Indicators and Warnings.** Indicators and warnings detect those actions of the enemy which are counter to planning assumptions. They there prevent the enemy from gaining surprise and allow the commander to initiate an appropriate response, such as a contingency, branch, or sequel operation.
- **Performing Intelligence Preparation of the Battlefield.** Intelligence Preparation of the Battlefield (IPB) is the US Army's doctrinal approach to understanding the battlefield and the options that it presents to friendly and enemy commanders. It will be examined in detail in a later lesson.
- **Performing Situation Development.** Situation development is, an extension of the IPB process. Essentially, it involves the intelligence staff overwatching the developing situation to make sure that their Intelligence Preparation of the Battlefield remains relevant to the commander. It does so through a process of monitoring indicators and warnings which confirm or deny the threat's adoption of a particular course of action.

- Perform Target Development and Support to Targeting. This task involves the identification of targets which are critical to the enemy's course of action (High Payoff Targets) and a further refinement of this list into targets that must be neutralized for the friendly mission to succeed (high Value Targets). Importantly, it also involves the establishment of procedures to pass information and intelligence from intelligence assets to the appropriate "shooter."
- Support Force Protection. Force protection identify, locate and target an enemies ability to target and affect friendly forces, facilities and operations.
- Perform Battle Damage Assessment. This intelligence task involves the assessment of the effects of both lethal and non-lethal measures taken against a target. It allows the commander to decide if conditions have been met to allow transition to another phase or operation or which targets, in what priority order, need to be re-engaged.

When performed correctly as part of a total force effort, these tasks allow the commander to apply and conserve his combat power by directing it quickly and accurately at his High Value Targets (HVTs).

Training the IEW BOS. The responsibility for training the IEW BOS lies with the commander. However, the G2(S2) assists the commander in developing realistic training which is integrated with the training of combat, combat support, and combat service support units. Conversely, MI personnel must understand the characteristics, tactics, and operations of the units that they are supporting so that IEW operations can be synchronized with the commander's concept of operations. Whenever possible, intelligence training should be relevant to the real-world intelligence requirements of the unit. Intelligence training should be derived from the unit's Mission Essential Task List (METL), battle tasks, and operations plan requirements. TCS 34-10-20, 34-10-20-1, and 34-20-20-2 contain standards by which METL can be developed, and training planned, executed and assessed.

The Levels of Intelligence. There are three levels of intelligence that correspond to the three levels of war: strategic, operational and tactical. The levels of intelligence are not tied to specific echelons but to the operations they support. The ground commander, regardless of echelon will be provided with a mix of all three levels of intelligence. Strategic intelligence may address the host nation's political climate or ethnic situation; operational intelligence identifies key enemy objectives for the campaign; and tactical intelligence reveals where and how the enemy can be decisively engaged and defeated. The three levels of intelligence are:

- Strategic. Strategic intelligence supports the formation of strategy, policy and military plans and operations at the national and theater levels. At the Strategic level, intelligence officers are concerned with the political, economic and military capabilities, vulnerabilities, and probable courses of action of foreign nations.
- Operational. Operational intelligence supports the planning and conduct of campaigns and major operations within a theater of war and serves as the bridge between strategic and tactical intelligence. At this level, intelligence officers are concerned with identifying the High Value Targets (HVTs), lines of communication, and other elements

necessary for campaign design. It focuses primarily on commanders from theater through corps and task force.

- **Tactical.** Tactical intelligence supports the execution of battles and engagements at corps level and below. It is the intelligence required by the commander to provide a basis for planning and conducting of tactical operations in support of the operational commander. It is perishable intelligence that usually emphasizes the environment and threat forces, and therefore has the ability to immediately influence the outcome of the commander's mission.

Intelligence Disciplines and Functions. Intelligence has four disciplines; human intelligence (HUMINT), imagery intelligence (IMINT), signals intelligence (SIGINT), measurement and signature intelligence (MASINT); and two multidiscipline functions: counterintelligence (CI) and technical intelligence (TECHINT).

HUMINT. HUMINT is the collection of information from human sources. It is usually used to confirm or deny intelligence derived from other disciplines. However, it can be the most important type of intelligence when conducting operations in a low technology environment, such as humanitarian assistance in a developing country.

IMINT. IMINT is the product from imagery analysis, including radar, infrared, and optical sensors. IMINT is often the primary source of intelligence for physical damage assessment during battle damage assessment.

MASINT. MASINT is the product from the analysis of objects or events from their signature. MASINT sources include lasers, radar, and magnetic and seismic sensors.

SIGINT. SIGINT is the product from intercepted communications and non-communications emitters. This includes the threat's command, maneuver, and fire control emitters.

CI. In essence, CI provides force protection. It is designed to defeat or degrade threat intelligence gathering capabilities, including enemy HUMINT, SIGINT, and IMINT capabilities.

TECHINT. TECHINT is the product which results from the analysis of foreign technical developments allowing US forces to identify or counter an enemy technological advantage.

Characteristics of Effective Intelligence. This lesson has emphasized that intelligence exists to support the commander in the successful achievement of his mission. Effective intelligence can be measured again by the following standards:

- **Timely.** Intelligence is useless unless it is produced and disseminated in time for it to support planning and influence decisions. It must get to the people who need to know it, when the need to know it.
- **Relevant.** Intelligence must support the commander's concept of operations and his mission. Relevancy is first established through the selection of appropriate Priority

Intelligence Requirements (PIR). The intelligence provided must also be in a usable format.

- Accurate. Intelligence officers must have moral courage. They must be prepared to present facts and assessments according to the battlefield environment and situation and not tailor their products to support a vision of what they or their commanders would prefer the enemy to be doing. Alternative or contradictory assessment should be presented, when necessary to ensure balance. Intelligence should be derived from multiple sources and disciplines to minimize the possibility of deception or misinterpretations.
- Predictive. Intelligence is not historical. It allows the commander to seize and maintain the initiative by telling him what the enemy is doing, can do, and how they are most likely to attempt this course(s) of action.

The Intelligence Cycle. Intelligence is a key element of combined arms operations. It enables commanders to use their combat power effectively and efficiently to win the decisive battles, by predicting what, where, when, why and how the enemy will attempt to conduct operations. The intelligence cycle is a tool used in intelligence operations to help the commander answer his intelligence needs. It is a continuous process consisting of five steps and driven by the commander's mission. The mission lies at the core of the intelligence cycle. Given a mission, a commander issues guidance to his staffs, who, in turn, transform this guidance into a concept of operations through the staff planning cycle. The mission and concept of operations help determine Priority Intelligence Requirements (PIR) and Information Requirements (IRs), which, as they are answered, impact on the commander's combat decisions. The five steps of the intelligence cycle are:

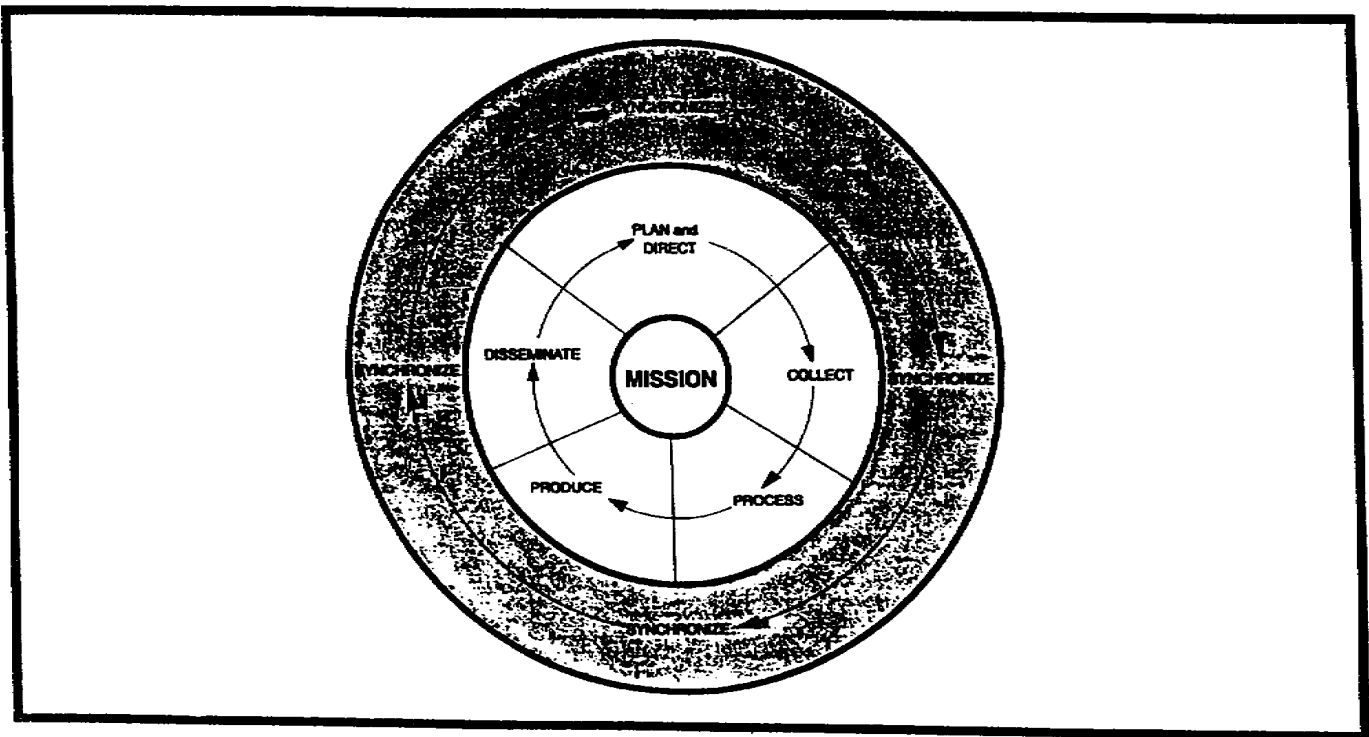


Figure 1-1. Intelligence Cycle.

- Plan & Direct. Commanders direct their intelligence operations through their G2 (S2). The G2 (S2) uses IPB as the primary tool to focus and direct all of the phases of the intelligence cycle. During this phase MI assets will be task organized, intelligence requirements and priorities will be developed, a collection plan is developed to answer the commander's PIRs and IRs, and units are tasked. It is important to remember that it is the Commander who drives intelligence not the G2 (S2). As this is the phase where PIRs and IRs are determined, it is appropriate to define these two terms:

*PIR. An intelligence requirement associated with a decision that will affect the overall success of the command's mission. PIRs are prioritized among themselves. This priority may change according to the situation.

*IR. An information requirement of lower priority than the PIR of the lowest priority.

- Collect. During the collection phase, information is acquired by the tasked sources and agencies and distributed to the processing and production elements. It includes the maneuver and positioning of intelligence assets to locations favorable to satisfying collection objectives.
- Process. Processing is the conversion of collected information into a suitable form for the production of intelligence. It includes the development of film, the translation of foreign documents and the automated processing of information that occurs within the All Source Analysis System (ASAS). Effective processing will ensure that relevant information is extracted in a timely, prioritized manner.
- Produce. This phase of the intelligence cycle involves the integration, evaluation, analysis, and synthesis of information into intelligence. At the tactical level, time constraints will tend to make phases three and four indistinguishable. Implied in this phase is the use of several aids, including:
 - Evaluation devices such as order of battle files and source profiles.
 - Analysis devices such as situation maps, templates, and doctrinal manuals.
- Disseminate. This is the final phase of the intelligence cycle. Disseminate. Dissemination is the timely distribution of intelligence in a usable form to the appropriate decision maker. Dissemination methods can include: personal contact, such as briefings; and intelligence documents, such as estimates, summaries, reports, and the Intelligence Annex to an Operations Order. The diversity of forms and means requires interoperability among command, control, communications, and intelligence (C3I) systems.

LESSON 1

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. Which of the following are part of the six tasks of IEW?
 - A. Provide indicators and warnings, perform IPB, and be timely, accurate, relevant and pertinent.
 - B. Perform IPB, perform the intelligence cycle, and conduct split-based operations.
 - C. Perform situation development, support the commander, and perform IPB.
 - D. Perform battle damage assessment, perform target development and support to targeting, and support force protection.

2. When is information converted into intelligence?
 - A. When information is broadcast to multiple echelons to achieve a common picture of the battlefield it is manipulated by organic intelligence staffs to become intelligence.
 - B. During the "produce" phase of the intelligence cycle.
 - C. When it is timely, relevant, accurate, and pertinent.
 - D. The conversion of information into intelligence is a continuous process that takes place during IPB.

3. Which of the following would most probably be the best source of intelligence for US forces escorting food convoys in an African country?
 - A. Intercepted radio traffic from government and factional propaganda stations.
 - B. Analysis of the equipment used by bandit groups, particularly their "technical" style vehicles.
 - C. Interviews with towns people living along the projected supply routes.
 - D. Imagery of the towns along projected supply routes.

LESSON 1
PRACTICE EXERCISE
ANSWER KEY AND FEEDBACK

| <u>ITEM</u> | <u>CORRECT ANSWER AND FEEDBACK</u> |
|-------------|------------------------------------|
| 1. | D. Page 1-2 or 1-3. |
| 2. | B. Page 1-6. |
| 3. | C. Page 1-4. |

LESSON 2

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

Critical Tasks: 301-372-2050
301-372-2051
301-372-2052
301-372-2053
301-372-2054
301-372-2055
301-372-2056
301-372-2057

OVERVIEW

LESSON DESCRIPTION:

This lesson will provide you with the tools necessary to understand and conduct the primary functions of the intelligence officer; analysis. Intelligence Preparation of the Battlefield (IPB) is a systematic, continuous process of analyzing the threat and environment in a specific geographic area. It integrates information on the enemy, weather and terrain, providing the basis for situation development, target value analysis, collection, reconnaissance and surveillance planning, and battlefield decision-making.

TERMINAL LEARNING OBJECTIVE:

- TASKS:** Be able to explain and perform the IPB process.
- CONDITIONS:** You will be given narrative information from FM 34-130.
- STANDARDS:** As a result of this lesson, you will, in an all-source intelligence environment, be able to perform the functions of the IPB process, and to develop its written and graphic products.
- REFERENCES:** The material contained in this lesson was derived from the following publication:

FM 34-130

INTRODUCTION

The complexity, intensity, and lethality of modern warfare makes battle command a difficult task. Intelligence personnel and their systems provide the commander with information concerning the threat, weather, and terrain and the effects of these factors on threat and friendly courses of action (COA). IPB ensures that intelligence personnel undertake this task in a thorough, uniform manner.

IPB is a four step process as shown below:

Step 1 -Define the Battlefield Environment. The first step of the IPB Process is Define the Battlefield Environment. Defining the Battlefield environment involves identifying for further analysis, specific features of the environment, or activities within it, and the physical space where they exist, that may influence available COAs or the commander's decisions. In general terms, this step is an overview of the situation facing the commander, and it focuses the remainder of the IPB process. A summary of this step is as follows:

- Identify significant characteristics of the battlefield environment.
- Identify the Area of Operations (AO) and battlespace.
- Establish the limits of the Area of Interest (AI).
- Identify the amount of detail required and time available for IPB.
- Evaluate existing databases and identify intelligence gaps.
- Collect the material and intelligence required to conduct the remainder of IPB.

Three important concepts in this step are as follows:

- The AO is defined as that portion of an area of conflict necessary for military operations. AO are geographical areas assigned to commanders for which they have responsibility and in which they have the authority to conduct military operations. The assigned AO is based on the factors of mission, enemy, terrain, troops, and time available (METT-T) and must be of sufficient size to allow completion of the assigned mission. Commanders at each level are normally assigned AOs which extend beyond the Forward Edge of the Battle Area (FEBA) or attack objectives, a distance commensurate with their unit capabilities. The G2 (S2) evaluates the mission and the assigned AO and together with the rest of the staff, recommend the AOs for subordinate units.
- The Battlespace is a physical volume that expands or contracts in relation to the ability of a commander's assets, or those acting on his behalf, to acquire and engage the threat. It does not necessarily include all of the commander's AO and, conversely, it may extend beyond that AO, depending on the breadth, depth and height in which the commander has positioned and moved his assets over time.
- The AI is the geographical area from which information and intelligence are required to permit planning or successful conduct of the command's operation. The AI is usually larger than the command's AO and battlespace; it includes any threat forces or characteristics of the battlefield environment that will significantly influence accomplishment of the command's mission. The AI includes the AO and areas adjacent, forward, and behind it. Note that the AI is not assigned but its dimensions are recommended by the G2 (S2) based on METT-T, the commander's operational intent, and intelligence gaps or uncertainties. The Ai is approved by the commander.

Step 2 -Describe the Battlefield's Effects. The second step in the IPB process is Describe the Battlefield's Effects. This step involves the determination of how the battlefield environment

affect both threat and friendly operations. In this step, the G2 (S2) identifies the battlefield environment's limitations and opportunities for friendly and threat COAs. Describing the battlefield's environment is done in the following sub-steps:

- Analyze the battlefield environment by conducting:
 - * Terrain analysis.
 - * Weather analysis.
 - * Analysis of other characteristics of the battlefield, such as political, ethnic, or religious factors.
- Describe these effects on threat and friendly capabilities and COAs.

Terrain Analysis. Terrain analysis reduces the uncertainties of the effects of terrain on operations. In order to accomplish this, the intelligence staff at headquarters higher than divisional level receives support from a direct support engineer terrain team or detachment. The terrain team performs technical evaluation of the topographic considerations of relief and drainage, vegetation, and hydrology. The graphic product of all of these considerations is called the Combined Obstacles Overlay (COO). The team's products support the intelligence staff's analysis of the five military aspects of terrain, which are known by the acronym, OCOKA. OCOKA stands for: Observation and Fields of Fire, Concealment and Cover, Obstacles (man made and natural), Key Terrain, and Ground and air Avenues of Approach and Mobility Corridors. The graphic product of all of these considerations is called the Modified Combined Obstacles Overlay (MCOO). The OCOKA factors are analyzed in terms of the mission and type of the unit, the type of operation, the level of command, the composition of forces involved, and the weapons and equipment expected to be encountered. This detailed analysis determines those areas on the battlefield which hinder, and those which facilitate, friendly and threat abilities to move, shoot, and communicate.

Observation and Fields of Fire. Observation is the ability to see over a particular area to acquire targets. The words observation and visibility are often used interchangeably, however, this is imprecise. Visibility is weather dependent or is a temporary condition. Observation, on the other hand, is terrain dependent and is relatively permanent. Generally, the best observation is obtained from the highest terrain in an area. Fields of fire refers to the area a weapon can cover effectively from a given point. Fires can be of two basic types: direct and indirect. Direct fire weapons are machine guns, rifles, and weapons such as TOW, all of which require the shooter to be able to see their target. Indirect fire weapons, such as mortars and artillery, do not require the shooter to be able to see their target, and they are primarily affected by terrain conditions within the target area which influence the terminal effect of the projectile. A key thing to remember is that observation and fields of fire do not always equate to each other. You may be able to see 25 km, but if all you are armed with is a rifle, then your fields of fire will probably be limited to around 500 meters. Observation and fields of fire should always be briefed in terms of weapons ranges.

Concealment and Cover. Concealment is protection from observation, either from the air or from the ground, and is vital to operations security (OPSEC) and deception operations. An

element of the terrain that often provides concealment without providing cover is vegetation. Certain features of the terrain will provide concealment from both ground and aerial observation, while other features may provide concealment from only one of these. When you describe the military aspects of the terrain you need to be precise as to what type of concealment you are talking about. Cover is the protection from the effects of weapons fires; direct, indirect, and air to ground. Certain aspects of the terrain may provide good cover from some fires, while some may provide cover from only one of these types. Cover can also, in some cases, be used to protect a force from observation. If this is the case, then the object providing cover is also providing concealment. However, concealment and cover do not always equate.

Obstacles. An obstacle is any natural or manmade terrain feature that stops, impedes, slows, or diverts movement. Before a terrain feature can be called an obstacle, you need to know the characteristics of the unit which will move through the area, specifically how it is equipped, and its movement doctrine. If a terrain feature is an obstacle, there are specific aspects of that terrain feature which make it so. For example, a river may be an obstacle to tracked and vehicular movement for many reasons: steep banks, soft bottom, deep water, or swift current among them.

Key Terrain. Key terrain is a terrain feature (natural or manmade) which, if controlled, will give a marked advantage to whoever controls it. When a G2 (S2) briefs key terrain he must be prepared to justify why it has been chosen as such. Key terrain is dependent on echelon of command, mission, enemy, and the general situation. The commander may designate certain key terrain as decisive terrain if it will have an extra-ordinary impact on the mission. To designate terrain as decisive is to recognize that the mission depends on seizing or retaining this terrain. While key terrain gives a marked advantage to whoever controls it, decisive terrain gives a decisive advantage to whoever controls it. Key or decisive terrain must be controlled, not necessarily occupied, and this may be done through either fires or maneuver.

Avenues of Approach and Mobility Corridors. An avenue of approach is an air or ground route of an attacking force leading to its objective or to the key terrain in its path. These are considered for the AO first and then, time permitting, for the AI. Aircraft, like ground forces, employ avenues of approach. Avenues of approach (AA) are determined by first identifying mobility corridors and then grouping them into AAs. Mobility corridors are areas where a force will be canalized (forced to use) due to terrain considerations. Mobility corridors are analyzed according to the size of the element that can doctrinally maneuver in them. They are restricted by terrain and obstacles and classified as follows.

- Unrestricted. Unrestricted terrain is free of any restriction to movement, not requiring any enhancement to mobility. Examples are plains or savannah areas with scattered or widely spaced vegetation.
- Restricted. Restricted terrain hinders movement to some degree. Without some degree of mobility enhancement, units may have difficulty maintaining preferred speeds, combat formations, or transitioning from one formation to another. Examples are swamps for dismounted infantry.
- Severely Restricted. Severely restricted terrain severely hinders or slows movement in combat formations unless mobility is significantly enhanced. Examples include steeply

sloped, heavily vegetated, or densely built up areas.

Generally, the following guidelines are followed for determining maneuver categories of slope. Note that a 45 degree incline is also considered to be a 100% slope, that is it increases vertically one foot for every horizontal foot:

- Unrestricted: 0-30% slope.
- Restricted: 30-45% slope.
- Severely restricted: greater than 45% slope. A slope of 45% or greater makes tactical maneuver impractical. Certain types of vehicles, such as tanks, can negotiate slopes in excess of 45%, but cannot maneuver for combat while doing so. So, forces will exploit existing lines of communication for maneuver.

When terrain is analyzed as to how it support cross-country mobility it is classified using the terms of unrestricted, restricted and severely restricted. These are some general guidelines to use, but remember, each case is equipment, doctrine, and situation dependent. When analyzing terrain to classify it as unrestricted, restricted, or severely restricted, it is important to consider the size and type force that is expected to maneuver through it. For example, the definition of what is severely restricted terrain differs for a light infantry platoon and an armor platoon. Mobility corridors (MC) are depicted as shown in Figure 2-1.

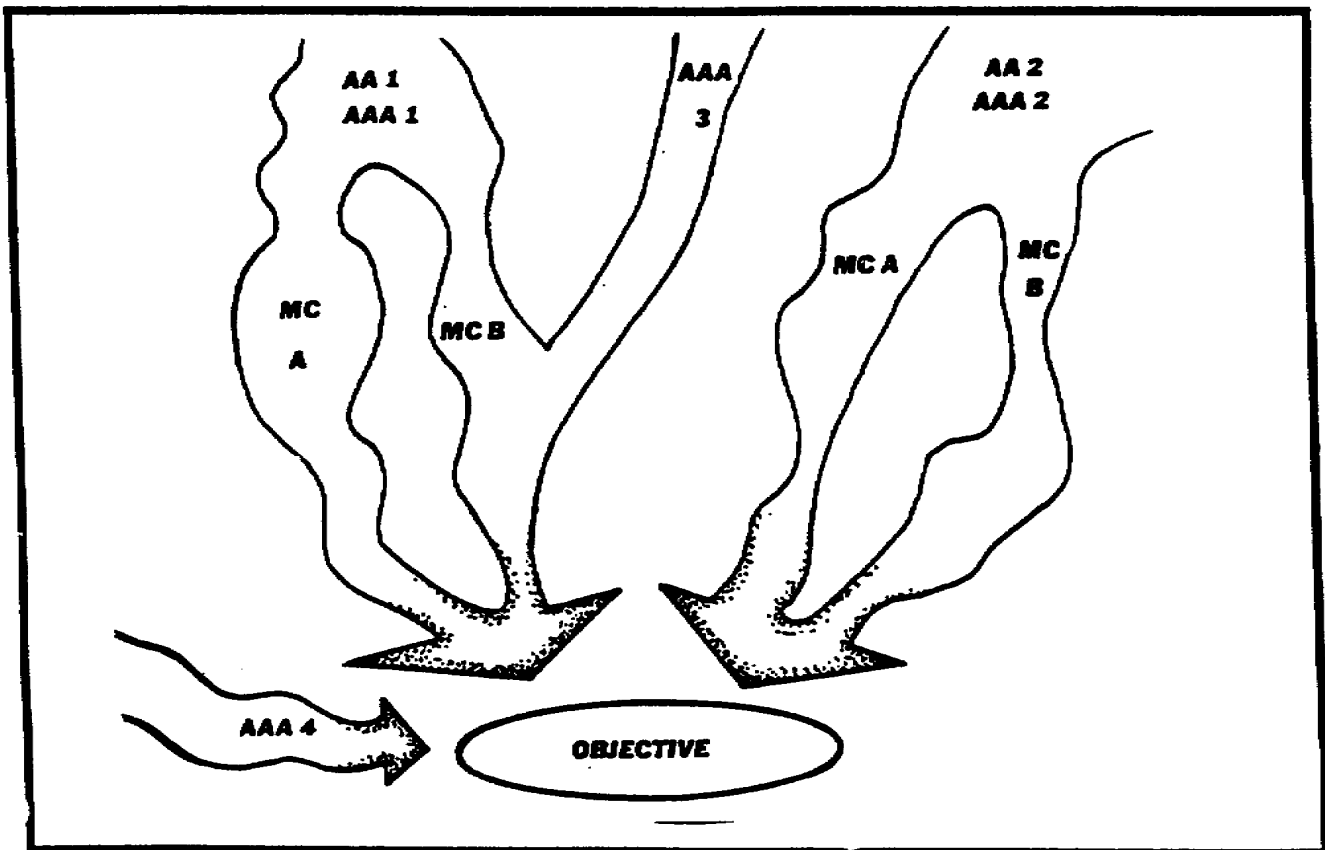


Figure 2-1. Mobility corridors.

The following Figure 2-2 shows the minimum width of mobility corridors for mechanized units. These figures apply to both friendly and threat units.

**Mobility Corridors
Minimum Widths
(Both Friendly & Threat)**

| | |
|------------------|--------------|
| Division | 6 km |
| Bde/Regt | 3km |
| Battalion | 1.5km |
| Company | 0.5km |

Figure 2-2. Mobility corridors minimum widths.

After examining the terrain or topographic considerations, we must consider the cumulative effects of all factors. In doing this we begin to graphically identify areas that will most likely and least likely be used for maneuver. We begin to apply analysis to the terrain factors to the critical aspects of terrain that will be useful to friendly and threat commanders. An example of what to look for in examining the cumulative effects of terrain factors would include analysis of the combined effects of slope and vegetation. Restricted terrain for slope combined with restricted terrain for tree spacing would most likely be severely restricted terrain. Another example would include examination of soil types with rain fall and drainage to determine if the terrain can be used for maneuver.

When analyzing the total effects of terrain on specific operations, the analyst uses the Modified Combined Obstacles Overlay (MCOO). These overlays are a total graphic representation of the critical military effects of terrain.

Identification of AAs and mobility corridors, which appear on the MCOO, provide a refined focus of our collection effort and intelligence analysis in Figure 2-1.

The next sub-step of Defining the Battlefield's Effects is weather analysis. When performing weather analysis, the intelligence staff has the support of weather experts in the form of the Staff Weather Office (SWO) provided by the Air Force. The SWO collates weather information collected throughout the battlefield and provides weather forecasts. The G2(S2) has overall responsibility for assessing how the effects of weather effect both friendly and threat operations. As the Army transition to Force XXI, weapons systems will become increasingly technical, and accurate weather information will become correspondingly more important.

The five military aspects of weather are: temperature and humidity, precipitation, winds, clouds, and visibility (see Figure 2-3). Intelligence staff must understand how combinations of different weather effects will influence operations. For example, restricted visibility can be beneficial to both offensive and retrograde operations as it provides concealment. While restricted visibility is generally considered to hinder defensive operations because reconnaissance and surveillance are impeded and target acquisition and engagement occurs at shorter ranges. A guide to the effects of weather can be found in FM 34-130, pages B-17 to B-22.

Temperature and humidity affect the operation of equipment and the efficiency of personnel.

Extreme temperatures, both high and low, can cause numerous problems such as a constant need for heated shelters, necessity for special clothing, equipment and combat skills.

Precipitation affects the state of the ground, visibility, personnel effectiveness, and the functioning of some equipment. A heavy rain may make some unsurfaced roads and off road areas impassable.

Wind speed and direction play an important part in operations scheme. Wind can effect the employment of equipment which uses antennas, it can reduce the effectiveness of GSRs by providing false returns. Apart from this, wind can also effect enemy and threat COAs by reducing the effectiveness of the down-wind military force by blowing dust, smoke, rain, or snow onto personnel and equipment. Additionally, wind has a dramatic effect on the employment of chemical and biological weapons, as well as the fallout pattern from nuclear explosions. One last effect of wind is its effect on personnel. Winds, by enhancing evaporation, increase the rate at which the body loses heat. The wind chill factor can increase the likelihood of cold injuries.

The type and amount of cloud cover as well as the height of the cloud base and tops, influence both friendly and threat air operations. Extensive cloud cover reduces the effectiveness of close air support. This effect becomes more pronounced as cloud cover increases, as cloud bases lower, and as conditions associated with clouds (icing, turbulence, and poor visibility aloft) increase. The ceiling is the height of the lowest layer of clouds covering 6/10th of the sky or more. Ceilings can affect temperature and the effect of nuclear weapons.

There are several factors which affect visibility including dust, haze, rain, snow, cloud cover during night, and light data. Light data considered by the G2 (S2) includes:

- Beginning Morning Nautical Twilight (BMNT) occurs when the Sun is 12 degrees below the horizon and rising. It is time when night lightens but the sun has not yet risen, also known as first light, and is the traditional time for the start of military operations.
- Sunrise occurs when the sun is at the horizon and rising.
- Sunset occurs when the sun is at the horizon and falling.
- End Evening Nautical Twilight (EENT) occur when the Sun is 12 degrees below the horizon and falling. It is the time when the sun has set but light still remains, also known as last light.
- Moon rise occurs when the moon is at the horizon and rising.
- Moon set occurs when the moon is at the horizon and falling. Note that Moon rise and moon set do now always occur at night.
- Percentage of illumination. Illumination relates to the percentage of the moon that is visible. For example, a 1/4 full, 1/2 full, and full moon would provide 25%, 50%, and 100% illumination respectively.

- Thermal crossover is a condition which can negatively impact the effectiveness of thermal sights. It occurs when the ground temperature is nearly equal to the temperature of the target. This does not always occur and the best way to determine if it will is to test it at your unit using your sights and vehicles.

| WEATHER EFFECTS | | | | | | |
|--------------------------------------|---|------------------------|------|------|------|------|
| FAVORABLE UNFAVORABLE MARGINAL | | GREEN RED YELLOW | 2400 | 0600 | 1200 | 1800 |
| VISIBILITY | EYE PASSIVE THERMAL | | | | | |
| | | | | | | |
| TRAFFICABILITY | FOOT WHEEL TRACK | | | | | |
| | | | | | | |
| AIR OPNS | ATTACK AVN AIR ASSAULT CAS UAV | | | | | |
| | | | | | | |
| | | | | | | |
| SMOKE OPSN | ENEMY FRIENDLY | | | | | |
| | | | | | | |

Figure 2-3. Weather Effects.

Step 3 Evaluate the Threat. The third step of IPB, is Evaluate the Threat. Evaluating the threat is conducted at the same time as the previous functions and involves a detailed examination of the threat. The intelligence staff analyzes all available information about the threat and try to think "red," like the threat commander. In doing so, the G2 (S2) will identify how threat forces normally conduct operations, as well as the threat's critical capabilities and vulnerabilities for his own commander. This step of the IPB process can be summarized as follows:

- Update or create threat models.
- Identify threat capabilities.

One of the key elements of evaluating the threat is the construction of templates. A template is a graphic representation of a threat's doctrinal capabilities drawn to scale as a map overlay (see Figure 2-4). A complete threat model consists of a graphic depiction, a written (usually bullet) description, and a description and identification of threat High Value Targets (HVTs). The threat template is used as a comparative data base to integrate the threat with the environment.

Templates may portray a variety of threat characteristics such as the disposition of forces, weapons, equipment, and fortifications. Functional systems, such as artillery or engineers, also may be templated. The nature of templates is such that they can be added to, changed, or deleted as the situation dictates.

A doctrinal template depicts the threat doctrinal deployment for various types of operations without the constraints imposed by weather and terrain. Composition, formation, frontages,

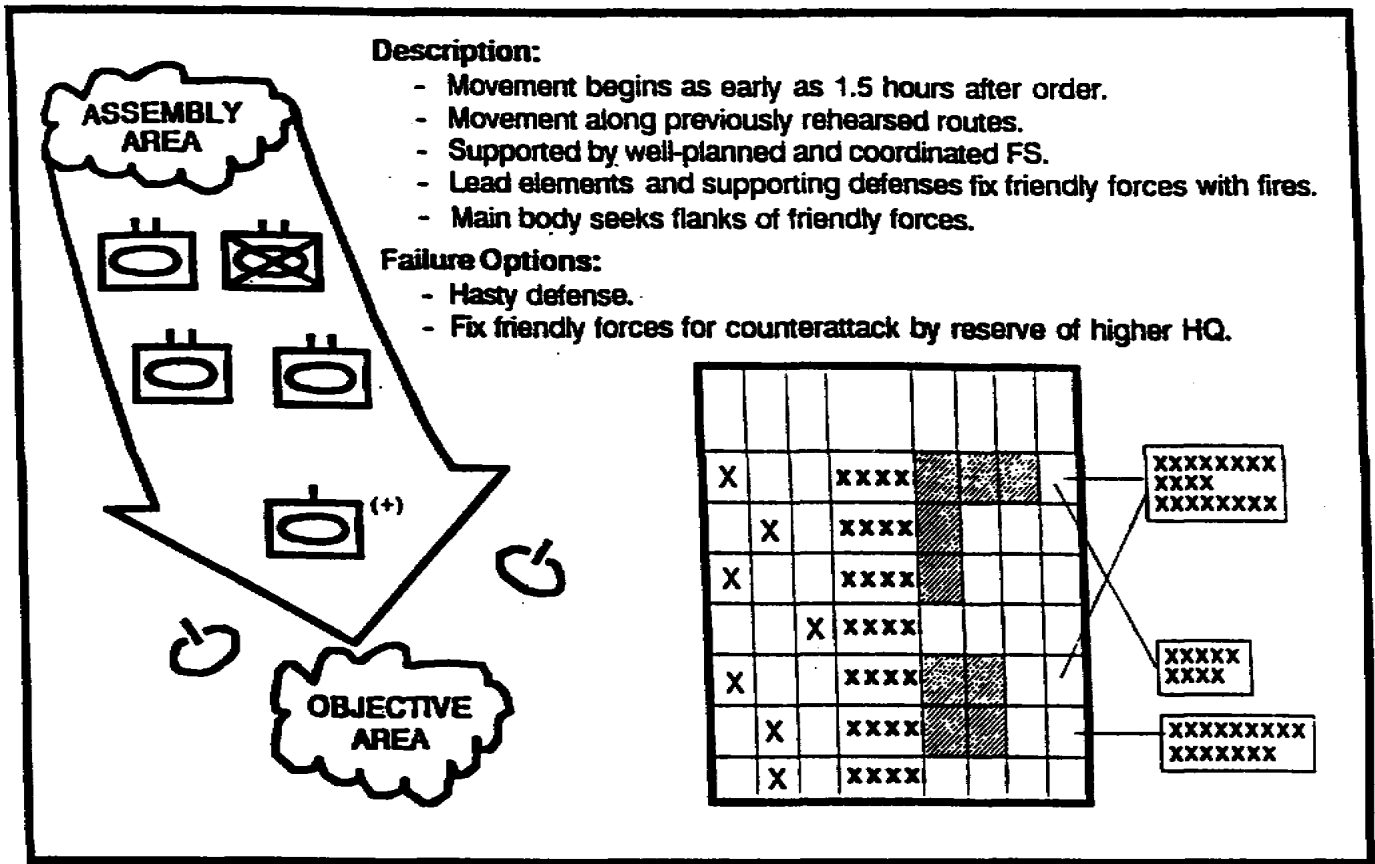


Figure 2-4. Threat Model.

depths, equipment, and HVTs are types of information displayed. What is templated depends upon the needs of the analyst.

Doctrinal templates help confirm suspected threat locations by helping you decide where to look with your limited collection assets. They assist in identifying gaps in OB just as a line and block chart of the threat would. Essentially, when doctrinal templates are compared to an OB database, an analyst can see what elements of the threat force have not yet been located, and, more importantly, help him assess their likely locations. They also constitute a graphic depiction of indicators so an analyst can spot deviations from doctrine and anticipate threat actions. While you evaluate the threat, you also identify critical threat assets for the commander, which are HVTs. HVTs are assets that the threat commander requires for successful completion of a COA. They are often from a non-maneuver BOS, and their value to the threat COA is likely to change depending on the phase of the operation. HVTs are ranked in importance, recommended by the G2 (S2) and approved by the commander. Examples might include command and-control, and communications elements, fire support elements, reserves, bulk fuel and ammunition sites, and air defense elements. There are a subset of HVTs called High Payoff Targets (HPT) which are a target whose loss to the threat will contribute to the success of the friendly COA. In other words, HPTs are threat HVTs which are developed and recommended by the staff and approved by the commander during wargaming and development of the Decision Support Template.

One of the evolving tasks of the intelligence staff which will assist in this step of IPB is the conduct of Order of Battle (OB) analysis. OB analysis involves determining the identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. This OB data is not normally furnished the commander. Instead, he is provided conclusions, estimates or analysis of probable threat COAs based on collated OB information. OB analysis includes the following categories of information:

- Composition is the identification and organization of units. Unit identification is often called the key to OB because it provides the answers to many questions concerning the threat. Through identification, the OB analyst is able to develop a history of the composition, training, tactics, and combat effectiveness of a threat unit.
- Organization is the structure of a unit and the relationship of the various echelons within the structure. Threat capabilities are difficult to assess accurately without knowledge of the current organization.
- Disposition provides intelligence about the location of threat units and the manner in which these units are tactically (or administratively in time of peace) deployed. In addition, disposition includes the recent, current, and proposed movement of threat units. Tactical deployment is the relative position of units with respect to one another or to the terrain. Tactical formations are designed for executing certain maneuvers. If this deployment can be determined, it may lead to an accurate appraisal of probable threat COAs.
- Strength is a description of a threat unit or force in terms of personnel, weapons, and equipment. Strength data is often expressed to the commander as a percentage of the threat unit that remains combat effective.
- Tactics include tactical doctrine as well as tactics employed by specific units. From a knowledge of tactical doctrine, the analyst knows how the threat may employ his forces in certain terrain and in order to achieve specific missions.
- Individual and unit training can significantly contribute to the combat effectiveness of any military organization. Each type or phase of training accomplished by a unit adds to its capabilities and effectiveness. Therefore, the combat effectiveness of a threat unit is more easily appraised when the degree and quality of its training are known.
- Logistics is also related to combat effectiveness. The adoption of a course of action is influenced by the ability of the logistical system to support that action. Some types of logistic information include:
 - * All classes and types of supplies.
 - * Requirements.
 - * Procurements.

- * Distribution.
- * Transportation.
- * Maintenance.
- Combat effectiveness is a term used to describe the abilities and fighting quality of a threat unit. Combat effectiveness affects the capabilities of a unit and may be predicted by analyzing such factors as:
 - * Personnel strength.
 - * Amount and condition of weapons and equipment.
 - * Status of training.
 - * Past performance. Unit history includes information and intelligence on component elements of a unit; on present and past parent units; and other details such as past performance and activities. Development of unit history is important because it aids in determining the capabilities and limitations of a unit.
 - * Personality traits of key personnel. This information is valuable because the tactics and combat efficiency of particular units are closely related to key individuals.
 - * Geographical area in which committed.
 - * Morale, health, discipline, and political reliability.
- Tech Data includes all of the technical information required by MI units to exploit SIGINT targets.
- Miscellaneous data includes various types of supporting information needed by an analyst to contribute to the development of the other OB element.
- Once threat models have been updated or created, depicted graphically, and HVTs have been identified, threat capabilities are identified through statements which reflect the broad threat COAs and supporting operations which might influence the accomplishment of the friendly mission. Examples of these statements include:
 - The enemy has the capability to attack with up to 8 divisions supported by 170 sorties of fixed-wing aircraft.
 - The enemy has the ability to covertly insert 2 battalions of light infantry by air into the corps rear area over a 12 hour period.
 - The enemy has the ability to seize objectives no deeper than the SOCHATON- MESSVILLE line due to insufficient fuel reserves.

Step 4 -Determine Threat Courses of Action. The final step of the IPB Process is Determine Threat Courses of Action (COA). This step integrates all previous steps to provide a clearer picture of threat intent and to provide graphic decision aids to the command and staff. The Intelligence Officer starts the process by thinking RED, and hypothesizing the various threat COA. In doing so he:

- Identifies the threat's likely objectives and end-state.
- Identifies the full set of COAs available to threat.
- Evaluates and prioritizes each COA.
- Develops each COA as time allows.
- Identifies initial collection requirements.

The consideration of likely threat COAs should incorporate all of the environmental, doctrinal, and threat model factors previously identified in the IPB process. COAs should be evaluated to make sure that they are suitable for achieving the threat's desired end state, feasible given time and resource constraints, present an acceptable risk, and be consistent with threat doctrine. Each considered COA should be significantly different from others that are considered and should include "wildcard" COAs which the threat may employ to achieve surprise.

These COA are similar to the threat models in that they consist of a graphic depiction of the COA, a description of the COA (Including options and branches), and a HVT list. The most significant difference is in the graphic depiction, which is done using a situation template:

- **Situation Template.** A modified threat doctrinal template which includes the effects of terrain and the environment and is constructed for a critical point in a COA. The situation template is produced by placing a doctrinal template over a selected mobility corridor or specific terrain and assessing how the threat force must modify its doctrinal configuration to account for environmental constraints. In essence, the analyst uses military logic to fit the threat force to the terrain as closely as possible. Situation templates should be developed for each critical event identified on the battlefield. For example, river-crossings are critical events, as are initial development positions, actions at the FLOT or FEBA, or passage of lines. In addition, situation templates may also be developed along avenues of approach and/or mobility corridors, since this is where we can most reasonably expect the threat to operate. This helps the analyst predict what the threat forces will look like at the instant they arrive at threat point on the battlefield. As threat forces move, their actions continue to be influenced by the environment, and the tactical situation. Since this movement is sequential, situation templates are also sequential, and can be considered to be "snapshots" of how the threat force might appear as it moves. As previously stated, the situation template is a modified doctrinal template which includes environmental constraints. The analyst will plot threat units on an overlay based on logical use of terrain while maintaining doctrinal frontages and depths where possible. Apart from the inclusion of environmental factors, the situation template should also include:

* Time Phase Lines (TPL). TPL depict expected movement of threat forces, such as in the advance, as reserves deploy, or in rear areas. TPL assist in predicting threat movements according to time and assist the collection manager in directing collection assets to named areas of interests (NAIs) when the threat indicators are likely to be there. TPL can be computed for all types of threat movement and operations, and can be utilized in the deep battle area to monitor movement along lines of communication, in the close-in battle to monitor actual threat operations, and in the rear battle to monitor the movement of enemy airborne/air assault or operational maneuver group forces towards their objectives. TPL are based on doctrinal rates of movement. These rates of movement are based on threat doctrine, operational experience, or on peacetime wargaming. Movement rates are adjusted to compensate for the effects of weather and terrain and for friendly actions. During operations, TPL are adjusted to conform to actual threat rates of movement.

* Named Areas of Interests (NAIs). The analyst assesses where threat activities that will best answer the commander's PIRs and IRs will occur on the situation template (see Figure 2-6). These become NAIs. A NAI is a geographical area where information that will satisfy a specific IR can be collected. NAIs can be a specific point on the ground (such as a crossroads or bridge), a specific movement route (such as a road or river), or an area. When possible, NAIs are placed in numbered sequence along an avenue of approach or mobility corridor. This facilitates the calculation of movement times between specific NAI, and limits confusion as the specific avenue or corridor under consideration. NAIs facilitate intelligence collection, reconnaissance, and surveillance asset employment and intelligence analysis because:

** They focus attention on areas where the threat force must appear if it has selected particular mobility corridors.

** They delineate when and where the enemy will employ his collection, reconnaissance and surveillance, fire support, and counterattack elements during friendly offensive operations.

** They frame militarily significant events by time and location.

** Events or activities in one named area of interest can be compared with events occurring at NAI in other mobility corridors to provide a basis for determining threat intentions.

** Events within NAI can be analyzed for indicators against which intelligence, reconnaissance and surveillance, and target acquisition assets can be directed.

Finally, the IPB process assists in the identification of initial collection requirements. The reason that intelligence is collected is to confirm which COA the threat has adopted by looking for indicators which support or deny each COA in specific NAIs. This is graphically represented in two products, the event template and event matrix.

- Event Template. The event template is a graphic portrayal of the differences between NAIs, indicators and TPLs associated with each COA. This equates to a collection and reconnaissance and surveillance plan in graphic form.

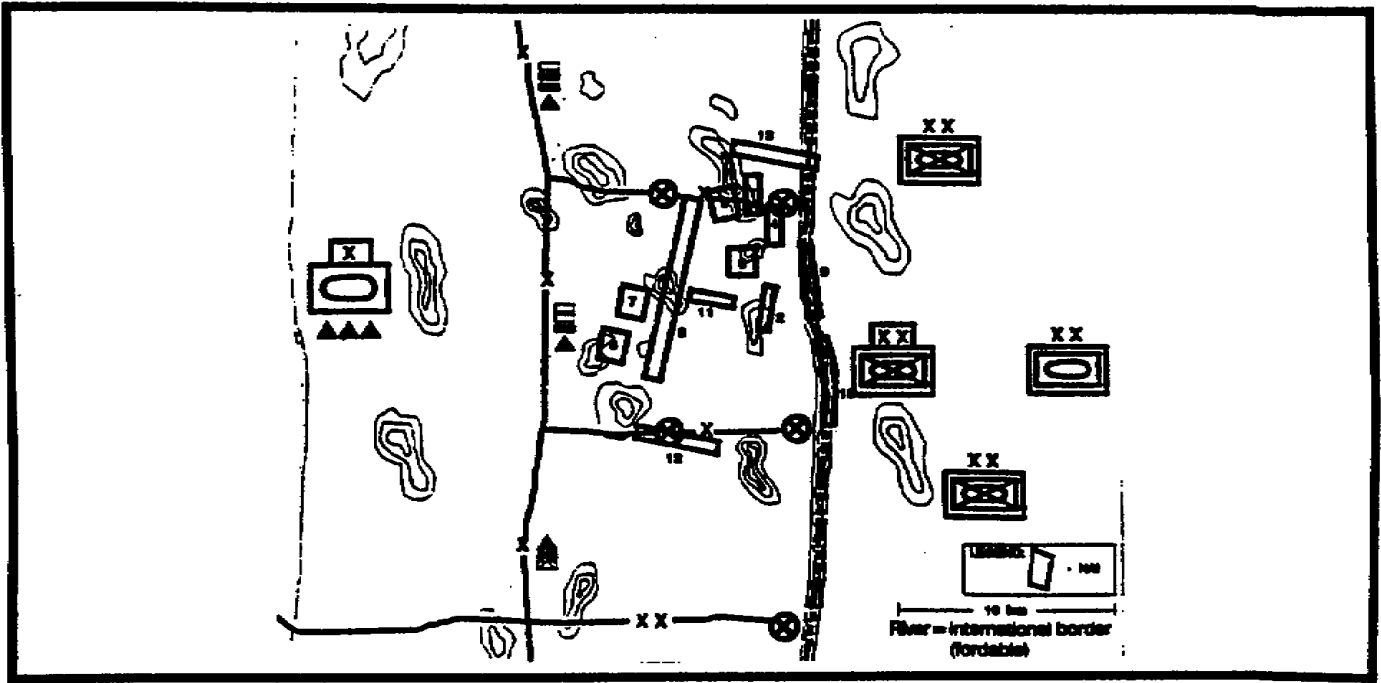


Figure 2-5. Event template/NAIs.

- Event Matrix. The Event Matrix further refines the event template by providing details on the type of activity to be expected, over time, in each NAI. These time "windows" are expressed in terms of no earlier than (NET) and no later than (NLT) times. This is an example of an event matrix (see Figure 2-6).

| NAI NO | NO EARLIER THAN | NO LATER THAN | INDICATOR |
|--------|-----------------|---------------|------------------------|
| 1 | H-7 | H-2 | Engr prep of arty posn |
| 2 | H-2 | H-30 min | Arty occupies posn |
| 3 | H-1 | H-15 min | Arty prep fire |

Figure 2-6. Event Matrix.

LESSON 2

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer to each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any question incorrectly, study again that part of the lesson which contains the portion involved.

1. During what step of the IPB process are situation templates developed?
 - A. Evaluate the threat.
 - B. Analysis.
 - C. Determine Threat COAs.
 - D. They are not developed in any specific step, but are produced concurrently with all steps.
2. What is a HVT?
 - A. A HVT is a threat asset that is required for successful completion of a threat COA.
 - B. A HVT is a threat asset whose loss to the threat will contribute to the success of a friendly COA.
 - C. A HVT is a threat non-maneuver BOS asset, such as bulk ammunition, or command and control elements.
 - D. A HVT is a threat asset, normally maneuver, that is depicted on the situation template.
3. NAIs are an important product of the IPB process because:
 - A. They are a geographical area where information that will satisfy a specific IR can be collected.
 - B. They frame militarily significant events by time and location facilitating intelligence collection, reconnaissance and surveillance asset employment, and intelligence analysis.
 - C. They allow the production of a consolidated situation template, and therefore analysis of where, when and in what manner threat forces will appear on the battlefield.
 - D. They are not important IPB product, being merely one of a suite of tools available to the intelligence staff to answer the commander's PIRs and IRs.

LESSON 2

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM

CORRECT ANSWER AND FEEDBACK

- | | |
|----|---------------|
| 1. | C. Page 2-12. |
| 2. | A. Page 2-9. |
| 3. | B. Page 2-13. |

LESSON 3

IPB AND ANALYSIS IN MILITARY STABILITY AND SUPPORT OPERATIONS

Critical Tasks: None

OVERVIEW

LESSON DESCRIPTION

This lesson will provide you with specific tools and skills to adapt the IPB process and conduct analysis in a Military Stability and Support Operations (SASO). It builds upon the knowledge and understanding gained from the IPB lesson.

TERMINAL LEARNING OBJECTIVE:

- TASK:** You will be able to conduct IPB in a SASO.
- CONDITIONS:** You will be given narrative information from FM 34-3, FM 34-7, FM 34- 130, FM 100-20, and FM 100-23.
- STANDARD:** As a result of this lesson, you will be able to, in an all-source environment to adapt the IPB process to SASO, and develop situationally appropriate written and graphic products.
- REFERENCES:** The material contained in this lesson was derived from the following publications:
- FM 34-3
 - FM 34-7
 - FM 34-130
 - FM 100-20
 - FM 100-23

INTRODUCTION

The range of operations which the US Army is likely to confront in the future is significantly greater than the arrow demands of conventional warfare. As the intelligence BOS supports the commander across the continuum of conflict, intelligence staff must be able to adapt to the commander's requirements in all situations. This lesson gives you the skills to do so.

SASO are conducted by the U.S. Army in its role as a strategic force to protect and further the interests of the U.S. at home and abroad in a variety of ways other than war. The definition of SASO is military activities during peacetime or in conflict that do not necessarily involve clashes between two organized forces.

This definition implies a special difficulty for intelligence staff. This is implied in the last phrase, "do not necessarily involve armed clashes between two organized forces." If threat forces are

not organized then it is difficult to do Order of Battle (OB) analysis and battle damage assessment against them. More importantly, if these forces do not clash militarily then the analyst is faced with the dilemma of trying to determine unfamiliar Courses of Action (COA) that do not revolve around military tactics.

U.S. Army doctrine holds that there is one IPB process for both conventional operations and SASO. However the IPB process is adapted for SASO:

"The IPB process in SASO is the same as in mid and high intensity conflict." FM 7-98.

"The principal difference between IPB for conventional battlefield situations and peace operations is the focus (on non-military topics) and degree of detail required (usually greater)." FM 100-23.

"The standard IPB process will work when applied to a SASO, but requires some alteration, primarily in focus and thought processes." FM 34-7.

"The four steps of the IPB process remain constant. The art of applying IPB to SASO is in the proper application of the steps to specific situations." FM 34-130.

The steps of IPB remain; Define the Battlefield environment, Describe the Battlefield's Effects, Evaluate the Threat, and Determine Threat COAs. The remainder of this lesson will provide you with the tools to properly apply these steps to specific SASO.

Define the Battlefield Environment. In this phase, the intelligence staff broadly identifies the characteristics of the battlefield which may influence friendly and threat operations. Following this, they should be able to identify intelligence gaps regarding these characteristics and identify the Battlefield Area, Battlespace, and Area of Interest. Ultimately, this phase focuses the remaining steps of the IPB process. In SASO, the intelligence staff should consider the following additional factors:

- Population.
- Economic and political systems.
- The Host Nation government and military.
- The nature of the threat to the commander's mission.

Describing the Battlefield's Effects. In this phase, the intelligence staff analyze the battlefield environment in detail by conducting terrain and weather analysis, and describing the effects of these factors on friendly and threat capabilities and COAs. In SASO, you consider the OCOKA factors as you would for conventional operations but it is here that you evaluate the population, which in SASO is generally considered to be the Key Terrain, and its lines of division.

Population Analysis. Population analysis includes the following:

- Lines of Division. The relevant lines of division in a population will be situation specific, but may include political, economic (including land ownership), racial or ethnic, religious, educational, health, welfare, and language. In addition, you should look at the effects that key personalities may have on friendly and threat capabilities and COAs through their influence on the population.
- Host Nation Government. The effects of any relevant factors concerning the Host Nation government should be analyzed, including: the governmental structures, parties and factions, special interest groups, key personalities, perceived legitimacy, and foreign policies.
- Host Nation Military. A similar process is gone through for the Host Nation military, including: the normal Order of Battle factors, including key personalities; the loyalty and affiliations of units and personalities to the government, lines of division within the population, and to the military leadership; and their ability to complete their mission.
- Based on these factors, the "worst case" of Host Nation military units operating against U.S. or coalition forces in a conventional setting should be considered.
- Miscellaneous. Finally, other miscellaneous factors should be considered. These will be highly situational but might include; population settlement or movement patterns for nomadic cultures, cultural taboos, third country historical political or economic interests, criminal activities and any other mission relevant factor.

As IPB is a graphically driven process, these relevant factors are most often depicted in the form of a number of graphics which may replace the traditional MCOO. There are SASO situations where a MCOO is relevant, such as where the threat includes conventional or semi-conventional forces, or where the activities of Host Nation or third party military forces are important. These SASO graphics will show any relevant factors, however, they typically include:

- Population Status Overlay (see Figure 3-1).

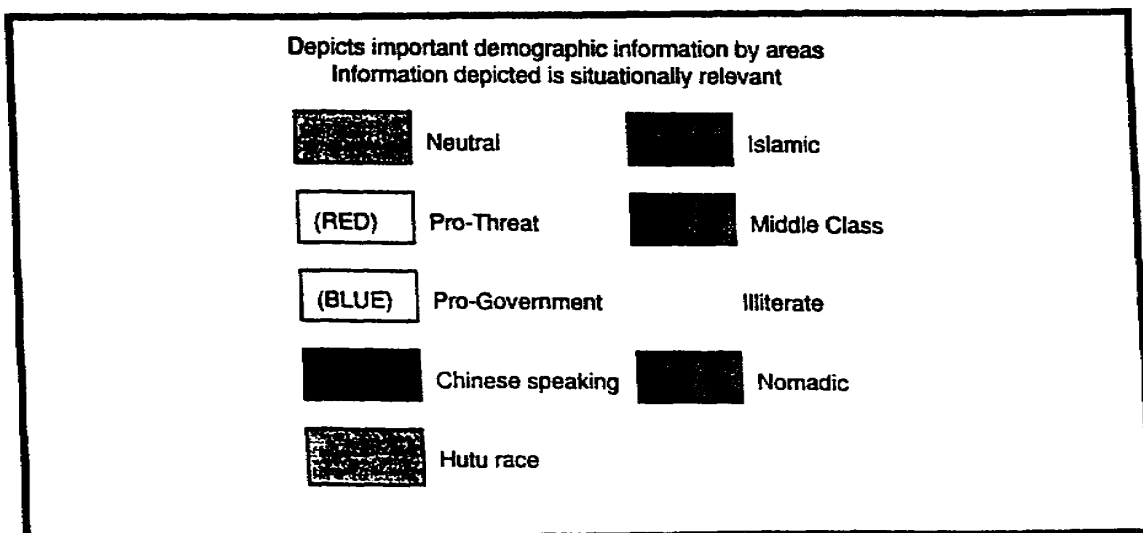


Figure 3-1. Population status overlay.

- Logistics Sustainability Overlay (see Figure 3-2).

LOGISTICS SUSTAINABILITY OVERLAY

Depicts those areas that provide threat sources of logistics, material, manpower and sustenance. Information is situationally dependent.

| | |
|---------------------------|--|
| Water | Gas/Fuel supply |
| Agricultural area | Drug processing chemical supply |
| Medical supplies | Machining facility |
| Medical facilities | Pro-threat schools |

Remember: It may require seasonal adjustment!

Figure 3-2. Logistics sustainability overlay.

- Concealment and Cover Overlay (see Figure 3-3).

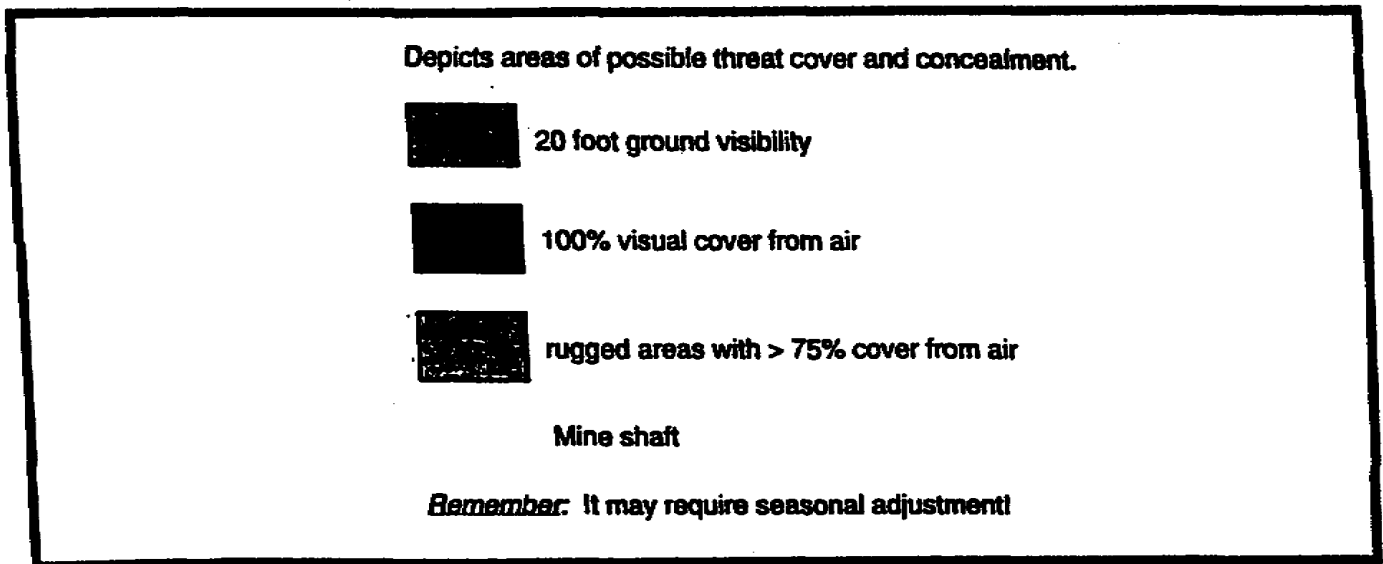


Figure 3-3. Concealment and cover overlay.

Lines of Communications (LOC) Overlay. Note that in certain situations, LOC will be different for a friendly and threat force (see Figure 3-4).

LINES OF COMMUNICATION OVERLAY

Depicts LOC that threat could utilize

Improved roads

Dirt roads

Trails

Sewer System, man navigable

Waterway, perennial, all watercraft navigable

Railroad

***Remember:* It may require seasonal adjustment**

Figure 3-4. LOC overlay.

- Key Facilities and Targets Overlay. Note that this overlay depicts what the threat is likely to target (see Figure 3-5).

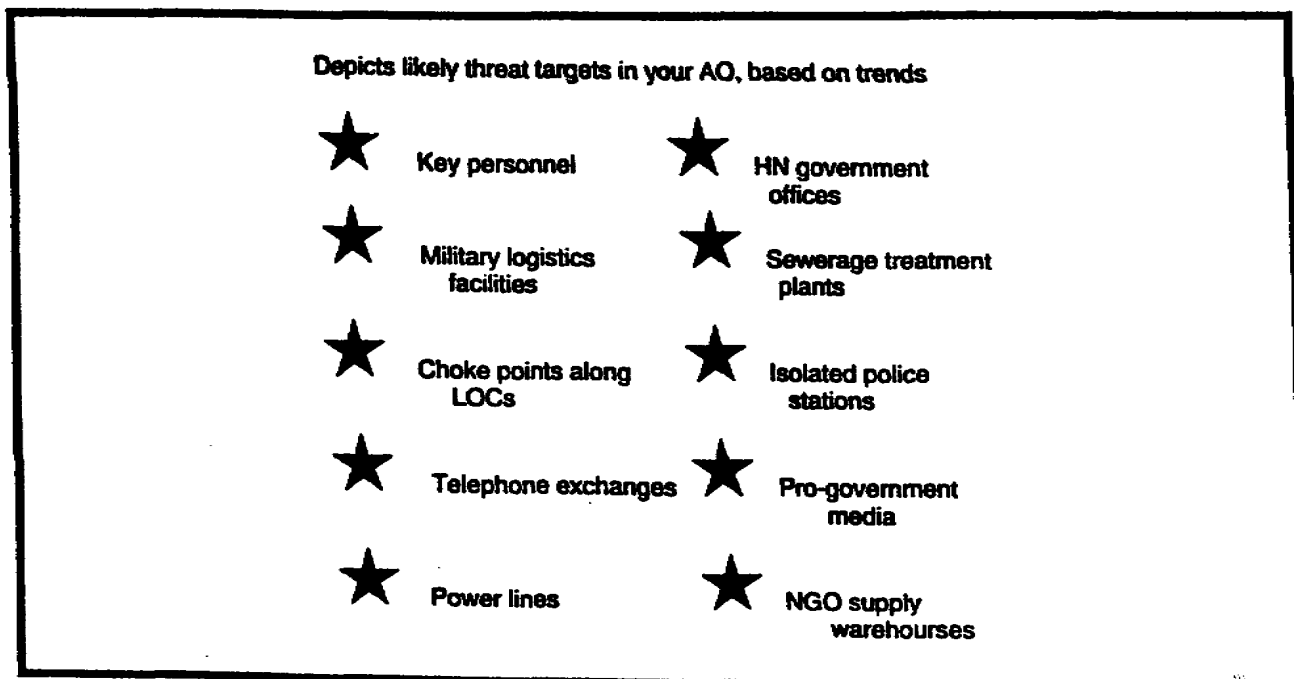


Figure 3-5. Key facilities and target overlay.

Examples of other, situationally relevant overlays might include Host Nation military dispositions and Host Nation police, correctional and judicial facilities.

Weather Analysis. Weather analysis for SASO does not differ greatly from that conducted in conventional operations. However, the effects of weather on SASO can be particularly significant. For example, consider the effects of rain on mass demonstrations or on a road trafficability for the delivery of humanitarian supplies; consider the affect of darkness of threat maneuver; and consider the effects of high winds on the aerial deployment of a friendly Quick Reaction Force. Because of these similarities the weather overlay remains the same, but a flexible mental approach is needed to ensure that the effects of the weather on friendly and threat operations are properly analyzed.

Evaluating the Threat. In this phase, the intelligence staff examine the threat in detail, converting threat doctrine into templates, identifying High Value Targets, and describing threat capabilities. There is no doctrinal definition of 'threat'. A suggested definition is 'any person, group, action or event that would cause a commander to fail to achieve his success criteria and therefore the mission.' The major difference between threat evaluation in conventional operations and SASO is that in the later, doctrinal templates are not used. Instead, threat operating patterns are determined, using historical data. These operating patterns, or modus operandi if you prefer, are able to be exploited during threat integration. Like in conventional operations, OB analysis is also done in SASO with the addition of the factor, key personalities. Once a reliable threat database is constructed, it will reveal if the threat has the capability to mount operations against the key facilities and targets previously identified. As a corollary of these threat capabilities, threat vulnerabilities are also implied. In terms of graphics this means that the doctrinal template is only used in SASO when appropriate, for example if the threat consisted of a ground attack squadron that might respond to a Marine show of force off the coast of North Korea, then doctrinal templates would be relevant. However, in general, doctrinal templates are replaced by operational pattern overlays and the process of constructing them is essentially one of reverse engineering. The basic information for operational pattern overlays comes from incident information, be it from an incident log or incident map. The data from these incidents is compared to the known threat OB data at the time of these operations to determine indicators and warnings. Lastly, other factors are considered, again, these will be situationally specific but might include such things as dates of historical significance (for example, the Tet offensive) and weather effects. Once these operational patterns are determined they can be fused with the key facilities and targets overlay to produce the equivalent of Decision Support Templates and Decision Support Matrices.

Determining Threat COAs. In the final phase of the IPB process, the intelligence staff 'think red.' They assess the threat's desired end state, identify all of the COAs available to them, evaluate each COA, and then develop them according to their assessed priority. This process also helps determine the initial collection requirements to confirm or deny each threat COA. The major difference in this phase between conventional operations and SASO is quantity. In the same way that there may be a multitude of hard to define threats in SASO, so may there be multiple COAs for each of these threat elements in reaction to each other, political or ethnic events, terrorism or other factors which fall outside the normal range of COAs considered in conventional operations (see Figure 3-6).

DETERMINE THREAT COAs

As there may be a multitude of these in Contingency Operations, each threat may also have multiple COAs.

| THREAT | COA |
|--------------------------------|---|
| each element of the population | in reaction to friendly operations |
| the HN military | in reaction to belligerent operations |
| third countries | in reaction to belligerent operations |
| each separate belligerent | in reaction to internal coalition differences |

Figure 3-6. Determine threat COAs.

Analysis in SASO. Once the IPB process has produced the threat COAs and helped determine collection requirements in order to confirm or deny them, the intelligence staff must be confirmed with making assessments from the information that they receive in order to turn it into timely and relevant intelligence which enables the commander to seize and maintain the initiative. It is during the processing stage of the intelligence cycle that this transformation occurs, and the focus of the remainder of this lesson.

Analysis determines the significance of information relative to what is already known about a threat or the battlefield environment, evaluates it, and draws conclusions from it which are related to the Commander's PIRs and the threat COAs. While we are talking about PIRs it is worthwhile mentioning that they tend to be more numerous in SASO, and can include nonmilitary information such as key threat personnel, the support for the threat within each line of division in the population, and past threat activity (to form the database for the operational patterns overlay).

Ultimately, the job of the analyst is to answer the Commander's PIRs. Again, analysis in SASO is similar to that conducted in conventional operations, but two additional techniques are emphasized; pattern analysis and link analysis:

Pattern Analysis. As previously stated, the threat in SASO can be quantified in terms of operational patterns or modus operandi. Pattern analysis identifies the common elements of threat incidents so that they can be identified as indicators and warnings. Here is a simple example of how pattern analysis might work:

You are conducting a Support to Domestic Civil Authority (SDCA) operation in a large city following a major earthquake. One of your Commander's PIRs is "to identify the areas where looting may take place." In similar circumstances in past natural disasters, looting has occurred in high-cost retail areas. In your SDCA AO there are nine such areas. So, how do you assess which of these areas is likely to be subject to looting? By

areas. So, how do you assess which of these areas is likely to be subject to looting? By using your IPB products. For example, by looking at your population status overlay you determine that the areas where looting has taken place have characteristically been within 3 miles of poor neighborhoods. In addition, from your adapted logistics sustainability overlay you see that these neighborhoods had not had water or electricity services reconnected at the time of the looting. You can therefore look at the nine areas in your AO and determine if any of them have similar circumstances, predicting to your commander that the high cost retail areas within 3 miles of a poor neighborhood which have not yet had basic services reconnected are likely to have looting incidents in their vicinity.

Link Analysis. We have emphasized that population is the key terrain in SASO and that key personalities are an additional factor in both the IPB process and in analysis. The following tools are used for analyzing the population, specifically key personalities:

- Association Matrix. The Association Matrix determines the degree of contact between individuals. In order to use this tool, you cross-reference the names of individuals and look at the degree of shading in the cross linked square. The more shaded the square, the greater the degree of contact between the individuals (see Figure 3-7).

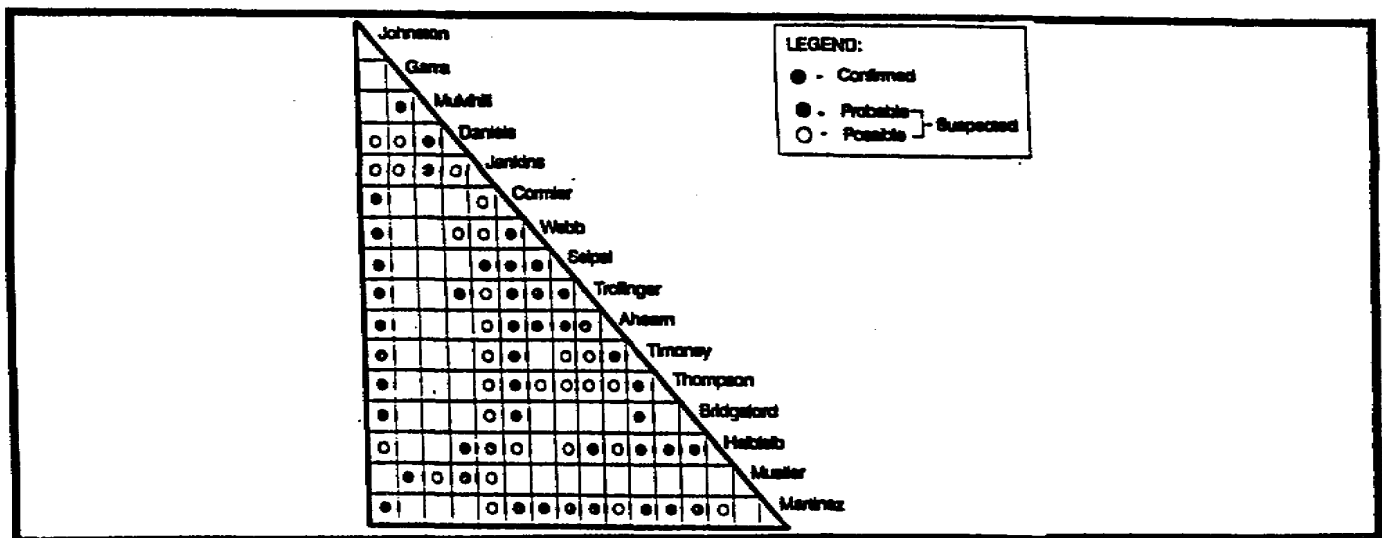


Figure 3-7. Association Matrix.

- Activities Matrix. The Activities Matrix determines the degree of relationship between individuals and activities. So while the Association Matrix can tell you that two individuals associate frequently, the Activities Matrix can tell you that they are probably engaged in, for example, propaganda activities. It is filled and read in the same manner as the Association Matrix except that it is a square rather than a triangular format (see Figure 3-8).

| LEGEND: | | Christian Reform Party (good guys) | Society for the preservation of order (right wingers) | Farmer's alliance (lunk peasant group) | People's Democratic Society (pacifist moderate) | Insurgent Company | New Liberation Movement (political front for N.M.E.) | N.M.E. | Name of individual | |
|---------------------|---|------------------------------------|---|--|---|-------------------|--|--------|--------------------------------|-----------|
| Remarks | | | | | | | | | | |
| Warrant outstanding | Leader in the insurgent co. Possible pit cdr or co cdr. | | | | | ● | ● | ● | Johnston, S.D. alias "The Red" | Bardolph |
| | Possibly linked to death squad activities. | ● | ○ | | | | | | Garr, N.A. | |
| | Mayor, ineffective due to war-torn town. | ● | | | | | | | Muhill, P. | |
| | Possible pit leader. | ○ | | ● | ○ | ○ | ○ | | Daniels, P. | |
| | Regional governor. | ○ | ○ | ○ | ● | | | | Jenkins, T.L. | |
| Warrant outstanding | Tactical genius, principal trainer of insurgent co. | | | | | ● | ● | ○ | Cornier, J. | Maconb |
| | | | | ○ | | ○ | ○ | ○ | Webb, C. | |
| | | | | | ○ | ○ | ○ | | Seipel, B. | |
| | Leader in the insurgent co. Pit leader or XO. | | | ○ | | ○ | ○ | ○ | Trolinger, L. | Beardtown |
| | Possible head of intelligence. | | | | | ○ | ● | ● | Aheam, E. | |
| | Probable pit leader. | | | | | ○ | ○ | | Timoney, J. | |
| Warrant | | | | | | ● | ● | | Thompson, J. | |
| Warrant | Probable hvy wpn pit leader. | | | | | ● | ○ | ● | Bridgford, R. | |
| | Possible liaison between insurgent co and the N.M.E. | | | ○ | ○ | ○ | | ○ | Hableib, M. | Bustment |
| | "Doctor of Death" leads the SPO. | ● | ● | ○ | ○ | | | | Mueller, H. | |
| Warrant | | | | | | ● | ○ | ○ | Martinez, E. | |

Figure 3-8. Activities Matrix.

- Time Event Chart. The time event chart is a tool which helps reverse engineer incidents to determine threat operating patterns. In this example, you can see that the insurgent winter offensive began with civil action, and escalated through terrorist activities to small scale attacks, while evidence of an increased logistics effort was discovered. This took place over a period of approximately one and half months. These, or similar incident patterns may be looked for in the future as indicators that another insurgent winter offensive is about to be undertaken (see Figure 3-9).

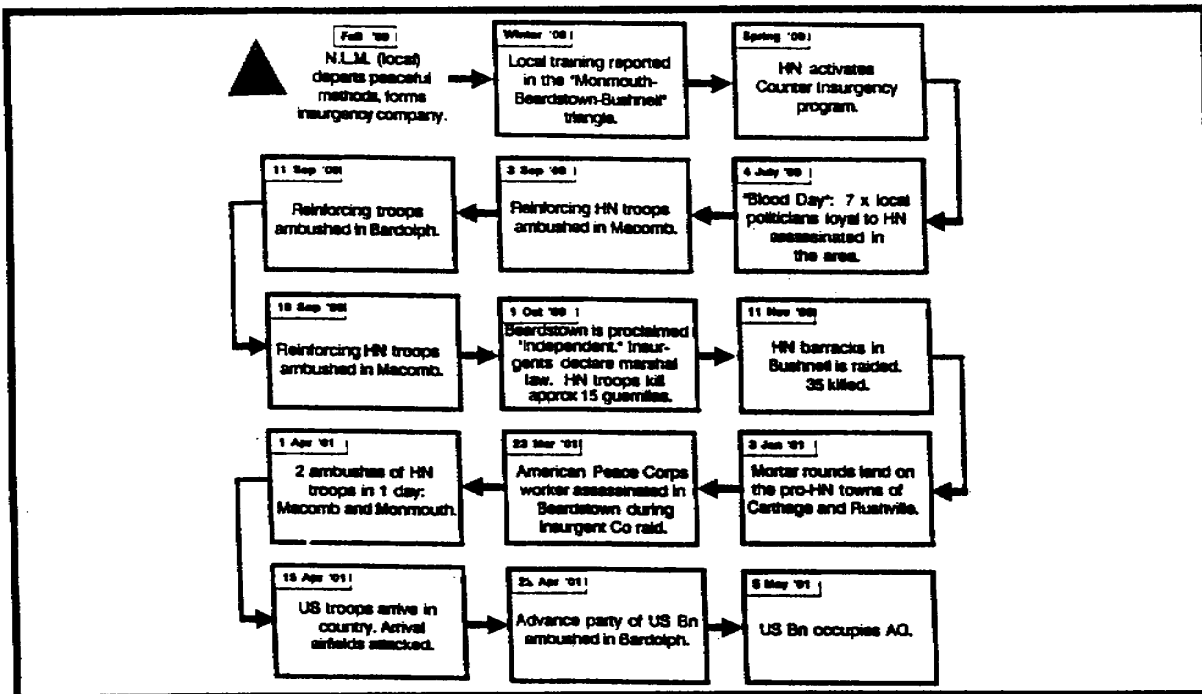


Figure 3-9. Time event chart.

- Link Diagram. The link diagram combines the association and activities matrices into a single graphic. It shows how individuals and functional groupings of individuals are related, allowing the determination of intelligence gaps and which threat individuals are critical to the functioning of the organization. From this later analysis, you can develop human High Value Targets (HVTs) for possible targeting according to Roles of Engagement (ROE). In the following example you can see that an intelligence gap exists on the connection(s) between the operational and CSS-equivalent elements of this terrorist organization. In addition, it appears that the individual associated with training is the most obvious HVT (see Figure 3-10).

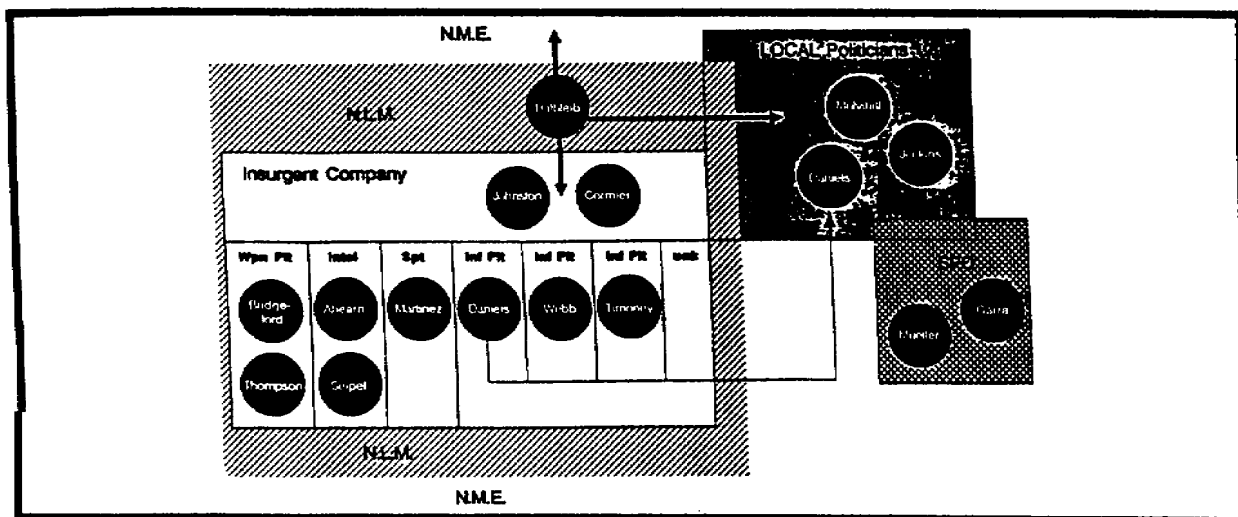


Figure 3-10. Link diagram.

LESSON 3

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer to each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any question incorrectly, study again that part of the lesson which contains the portion involved.

1. What is the most important difference between the IPB process in conventional operations and SASO?
 - A. There are no important differences between the IPB process in conventional operations and SASO.
 - B. Doctrinal templates are never feasible in SASO.
 - C. The IPB process requires a different focus and a greater degree of detail which results in an adaptation of the process to the specific situation.
 - D. Doctrinal templates and the MCOO are not usually required in SASO.

2. What is the major addition to the IPB step of terrain analysis in SASO?
 - A. The MCOO is replaced by the Population Status Overlay, the Concealment and Cover Overlay, the Lines of Communication Overlay, the Key Targets and Facilities Overlay, and the Logistics Sustainability Overlay.
 - B. The effects of weather on both friendly and enemy COAs must include considerations of appropriate cultural, ethnic and religious factors.
 - C. There is no major addition to this step, only adaptation of the OCOKA factors to the specific SASO situation.
 - D. Population analysis is done during this step.

3. What graphic products are produced by an analyst conducting link analysis?
 - A. The association matrix, activities matrix, and link diagram.
 - B. The association matrix, activities matrix, and pattern analysis overlays.
 - C. Pattern analysis overlays and time event charts.
 - D. The activities matrix, time event chart, and pattern analysis overlays.

LESSON 3
PRACTICE EXERCISE
ANSWER KEY AND FEEDBACK

| <u>ITEM</u> | <u>CORRECT ANSWER AND FEEDBACK</u> |
|-------------|------------------------------------|
| 1. | C. Page 3-2. |
| 2. | D. Page 3-2. |
| 3. | A. Page 3-8 and 3-9. |

LESSON 4

INTRODUCTION TO THE RESPONSIBILITIES OF THE GARRISON INTELLIGENCE OFFICER

Critical Tasks: None

OVERVIEW

LESSON DESCRIPTION:

This lesson will provide you with an introduction to the responsibilities and duties of the intelligence officer in garrison. It includes basic principles of physical security, information security, and information systems security.

TERMINAL LEARNING OBJECTIVE:

- TASK:** You will understand basic principles of garrison security programs.
- CONDITIONS:** You will be given narrative information from AR 190-11, AR 190-16, AR 190-51, AR 380-2, and AR 380-19.
- STANDARDS:** As a result of this lesson, you will be able to describe the basic principles of establishing a successful physical, information, and information system security programs.
- REFERENCES:** The material contained in this lesson was derived from the following publications:
- AR 190-11
 - AR 190-13
 - AR 190-16
 - AR 190-51
 - AR 380-5
 - AR 380-19

INTRODUCTION

The purpose of this lesson is to introduce you to one of many responsibilities of the intelligence office which fall outside the intelligence cycle and the IPB process.

Even though the Cold War has ended, the need to protect technology, information and sources in the U.S. Army still exists. The intelligence officer has the responsibility of protecting classified material, controlling dissemination of information and safeguarding sensitive items in times of war and peace. In garrison, the intelligence officer must maintain a high state of security awareness within the unit. The unit's physical security program will ensure proper storage and accountability of all weapons and sensitive items. The information security program will establish procedures for classifying and declassifying information, safeguarding and storage of

classified material, and proper destruction of classified information. An information system security program establishes guidelines for computer systems management, software control, computer accreditation and virus control.

Part A: Physical Security

Physical security can be defined as the part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage and theft. Physical security programs provide the means to counter threats during peacetime, mobilization, and wartime. The intelligence officer has the responsibility within the unit to establish and maintain an effective physical security program.

The intelligence officer has the primary role in the unit of designating Mission Essential vulnerable Areas (MEVA). MEVA consist of information, equipment property, and facilities which require additional protection through application of increased physical security measures, procedures, and equipment. The installation commander designates post MEVAs and ensures these areas are inspected and a periodic risk analysis is updated on these areas. The intelligence officer within the unit will designate the unit's MEVAs. A facility or area will be designated as MEVA if it is:

- essential to the accomplishment of the unit's mission;
- vulnerable to a threat that is intent on destroying, damaging, or tampering with property or equipment, including terrorism, or;
- vulnerable to a threat that is intent on removing protected items of equipment or property.

The MEVAs within your unit will be the primary focus of the physical security program. MEVAs must be designated in writing and forwarded to the installation commander for inclusion in the installation physical security plan. Some examples of areas to be considered are:

- Ammunition and explosive storage rooms, facilities or areas.
- Classified sites or location where classified material is stored.
- Command posts.
- Communications facilities.
- Consolidated supply and storage facilities.
- Motor pools and maintenance areas.
- Medical storage areas.

Physical threats to the unit's MEVAs can come from foreign intelligence services, terrorists, saboteurs, criminal elements or protest groups. The intelligence officer must implement programs to prepare for and counter these threats. The unit's physical security plan is a major portion of the unit's force protection. Measures that can be implemented within the unit can include but are not limited to:

- Security guards.
- Military working dogs.
- Physical barriers.
- Badging system.
- Locking devices.
- Security lighting.
- Surveillance systems.
- Access control devices.

Security guards can be implemented within your unit to control access to motor pools, arms rooms, ammunition storage areas or any area that needs continuous supervision and monitoring.

Military working dogs can be used to control areas surrounding the unit that are wooded or not easily observed. They can also be used to detect explosives or contraband within your area.

Physical barriers such fences with the minimum height of 6 feet tall that meet the requirements of U.S. Army Corp of Engineers Drawing Code STD 872-90-00. Series of perimeter walls over 6 feet high which delineate a boundary and serve as a barrier to personnel and/or vehicles can be used to control access into motor pools or secure areas.

A badging system which provides a security credential that is worn out on the possessor's outer garment and validates the person's authority for access to a restricted area can be used to control access to areas where classified material is stored or access to other sensitive areas.

Sensitive areas which cannot be observed 24 hours a day can be protected using high security padlocks with Military Specification MIL-P-43607. Locks however should be considered a delay device only, since any lock can be defeated by expert manipulation or force.

Security lighting can be used in conjunction with any physical security plan. It provides the amount of lighting necessary to permit visual surveillance by security personnel or anyone in the area into and around the sensitive area.

Surveillance systems are a combination of electronic components, including sensors, control units, transmission lines, and monitoring units integrated to be capable of detecting one or more types of intrusion into the area protected by the system.

Access control devices can be electronic badge systems, or guard shack which are the only way into or out of the sensitive areas. These devices restrict personnel and material going into or out of a restricted area.

These physical security measures will be implemented within the unit to protect and secure sensitive items and areas. Sensitive items within the unit can include:

- Weapons (mounted or dismounted).
- Ammunition.
- Classified material.
- Communication security (COMSEC).
- Night vision devices.
- Vehicles.
- Medical supplies.
- High value items (personnel property).

Part B: Information Security

Information Security. Technology and information relating to the national security will be protected against unauthorized disclosure as long as required by national security considerations. The Department of Defense (DoD) Information Security program establishes a system for classification, downgrading, and declassification of information. It also establishes policy and procedures to safeguard such information and technology. It is the policy of the DoD to make available to the public as much information as possible consistent with the need to protect the National Security. As an intelligence officer, your responsibility is to protect and safeguard the classified and sensitive information within your unit ranging from unclassified, confidential, and secret to top secret.

Confidential Information. Confidential information is information or material which the unauthorized disclosure could be expected to cause serious damage to the national security. Example of serious damage include disruption of foreign relations significantly affecting the national security or revelation of significant military plans or intelligence operations.

Secret Information. Secret information is information or material which the unauthorized disclosure could be expected to cause serious damage to the national security. Example of serious damage include disruption of foreign relations significantly affecting the national security or revelation of significant military plans or intelligence operations.

Top Secret. Top Secret information is information or material which the unauthorized disclosure could be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include armed hostilities against the U.S. or its allies, or disruption of foreign relations vitally affecting the national security.

Unnecessary classification and higher than necessary classification should be avoided. If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified "Confidential" pending a determination by an original classification authority who shall make this determination within 30 days. If there is reasonable doubt about the appropriate level of classification it shall be guarded as at the higher level of classification until a determination is made.

Classification Authority. Only the Secretary of Defense, the Secretaries of the Military Departments, and the Deputy Chief of Staff for Intelligence (DCSINT) will approve the delegation of TOP SECRET classification authority. Delegation of original SECRET and CONFIDENTIAL classification must be approved by the DCSINT.

Declassification. The declassification decision determines duration of protection, and is as important as the original classification determination. Those authorized to make original classification determinations must set a date or event for declassification if such a date or event can be predetermined as the time the original classification decision is made. The classification "Originating Agency's Determination Required (OADR) " is used only if the source document had OADR on it.

Need to know. A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, or knowledge, or possession of the classified information in order to accomplish lawful and authorized government purposes.

Marking Classified Information. Classified documents must be marked to show their classification and to ensure their proper safeguarding. Classification markings will be in letters larger than those on the rest of the page. They must be immediately noticeable to the reader. If the entire document is classified the classification will be at the top and bottom of the page both front and back.

Portion marking. Each section, part, paragraph, or similar portion of a classified document shall be marked to show the level of classification of the information contained in or revealed in it. If you portion a document, you must mark every section even if the section is unclassified. An example is as follows:

- (U) This is an unclassified sentence or paragraph.
- (C) This is a paragraph at the confidential level.
- (S) This is a section at the secret level.
- (U) This is an unclassified section.

These markings must continue throughout the entire document. The classification of this document which will be marked at the top and bottom will reflect the highest level of classification within the document. For the example, the document would be classified as Secret and safeguarded as such.

Destruction of Classified Material. Classified material and documents shall be destroyed by burning or, with the approval of the responsible DoD Component head or designatee, by melting, chemical decomposition, pulping, pulverizing, cross-cut shredding, or mutilation sufficient to preclude recognition or reconstruction of the classified information. In all cases, burning is the preferred method of destroying classified information.

Destruction Procedures. Destruction records and imposition of a two-person rule, that is, having two cleared people involved in the entire destruction process, will satisfy the requirements for Top Secret destruction. Imposition of the two-person rule, without destruction records, will satisfy the requirement for secret information. Only one cleared person needs to be involved in the destruction process for confidential information. The waste left over after the destruction should be checked thoroughly again to ensure no reconstruction of classified information is possible.

Information Security System. Information System Security (ISS) is the process of securing:

- Computer Hardware (terminals).
- Software.
- Terminal Procedures.
- Networks.
- Classified information in electronic form.
- Control of compromising emanations.

Vulnerabilities. Telecommunication or automated information systems (TAIS) and noncommunication emitters have inherent security vulnerabilities and are known to be targeted by foreign intelligence services. The need to secure these vulnerabilities is paramount to the intelligence officer.

Information System Security-Manager(ISSM). At all appropriate levels of command, an ISSM will be appointed to establish and implement the ISS program for all TAIS and communication emitters within that command.

Information System Security Officer (ISSO). For each TAIS there will be an ISSO appointed by the commander. The ISSO will:

- Ensure systems are operated and maintained according to regulations specified in AR 380-19.

- Prepare, distribute and maintain plans, instructions, guidelines and standing operating procedures (SOP) concerning the security of systems operations.
- Ensure a Terminal Area Security Officer (TASO) is appointed for each terminal or group of terminals not under the direct control of the ISSO.
- Prepare and oversee the preparation of the accreditation documentation.
- Report security violations and technical vulnerabilities to the ISSM.
- Terminal Area Security Officer (TASO). There will be a TASO appointed for each terminal or group of terminals to:
 - Issue written instructions specifying security requirements and operating procedures.
 - Establish each terminal user's identify, need to know, level of clearance and access authorization commensurate with the data available from that terminal.
 - Monitor local compliance with security procedures.
 - Report actual or suspected security violations to the ISSO.

Software Security. Safeguards implemented in software will protect against compromise, subversion, or unauthorized manipulation. Only software that has been specifically developed or approved for use, or has been purchased or leased by an authorized government representative is to spot check and ensure that "bootleg" software and pirated software is not being used. This activity could make TAIS vulnerable to manipulation or computer viruses.

Password Control. User identification and password systems support the minimum requirements of accountability, access control, and data integrity. These mechanisms while not always appropriate for stand alone small systems are most cost effective and efficient methods of achieving minimum security requirements. The ISSO oversees generations, issuance, and control of all passwords. The TASO may assist in issuing passwords in his or her respective area. All passwords should be generated by random generator software and must not be obtained from commonly used words or phrases. All passwords are maintained in writing by the ISSO and the TASOs.

Automated Information System Accreditation. Accreditation is the official management authorization to operate and TAIS or network and is based, in part, on the formal certification of the degree to which a system meets a prescribed set of security standards. The accreditation packet will show:

- The security environment surrounding the computer.
- The users of the terminal.
- The highest level of classification processed at the terminal.
- All software used on the terminal.

- All network capabilities of the terminal.
- Orders appointing the TASO and ISSO.
- All serial numbers, types and brands of hardware used.

Virus Protection. Computer viruses pose a serious threat to the ISS. All terminals must be monitored very closely for signs or symptoms' of viruses. However, with prevention being better than cure, measures must be taken to minimize the chance of infection of valuable data with viruses. One of the most common threats is the issue of unauthorized software or the sharing of infected disks. Both of these can result in a virus spreading throughout the unit and infecting numerous terminals. In the TAIS SOP, there must be specific guidelines set forth to be able to counter the virus threat to terminals.

LESSON 4

PRACTICAL EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer to each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any question incorrectly, study again that part of the lesson which contains the portion involved.

1. Which of the following would not be a MEVA?
 - A. An area or facility essential to the accomplishment of the unit's mission.
 - B. An area vulnerable to a threat that is intent on removing protected items of equipment or property.
 - C. Barracks.
 - D. Command Posts.

2. What classification of information would cause a serious damage to the national security if it were released to unauthorized agencies?
 - A. Confidential.
 - B. Secret.
 - C. Top Secret.
 - D. Unclassified.

3. Who is responsible for preparing and overseeing the preparation of the accreditation documentation?
 - A. ISSO.
 - B. TASO.
 - C. ISSM.
 - D. TAIS.

LESSON 4

PRACTICAL EXERCISE

ANSWER KEY AND FEEDBACK

ITEM

CORRECT ANSWER AND FEEDBACK

- | | |
|----|----------------------|
| 1. | C. Page 4-2. |
| 2. | B. Page 4-4. |
| 3. | A. Page 4-6 and 4-7. |